Exercices et problèmes

29 On considère les dix caractères A, B, C, D, E, F, G, H, I et J auxquels on associe dans l'ordre les entiers de 1 à 10.
On note $\Omega = \{1, 2, 3, ..., 10\}$. On appelle message tout mot ayant un sens ou non formé avec ces dix caractères.
Soit a un entier compris entre 1 et 10. On désigne par f l'application qui à tout élément i de Ω associe le reste de a^i modulo 11.

1. On suppose que a = 5.
a. Coder à l'aide de f le message « BAC » en utilisant la grille de chiffrement ci-dessous

Message	B	A	C
i	2	1	3
$f(i)$	3		
Code	C		

b. Coder à l'aide de f le message « FADE ».
Peut-on déchiffrer avec certitude le message codé ?
2. On suppose que a = 2.
Donner la grille de chiffrement de f.
Peut-on déchiffrer avec certitude un message codé?
3. On se propose de déterminer les valeurs possibles de l'entier a pour que l'application f permette de chiffrer et de déchiffrer avec certitude tous les messages.
a. Soit i et i' deux entiers compris entre 1 et 9 tels que $i < i'$. Montrer que
$a^i \equiv a^{i'} \pmod{11}$ équivaut à $a^{i'-i} \equiv 1 \pmod{11}$.
b. En déduire que f permet de chiffrer et de déchiffrer avec certitude tous les messages, si et seulement si, a^i n'est pas congru à 1 modulo 11 pour tout $i \in \{1, 2, 3, ..., 9\}$.
c. On suppose que k est le plus petit entier de Ω tel que $a^k \equiv 1 \pmod{11}$. Montrer que k est un diviseur de 10.
d. Conclure.

30 On considère la suite de Fibonacci $(F_n)_{n\geq 0}$ définie par $F_0 = 0$; $F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$, $n \geq 0$.
1. Calculer les termes de cette suite jusqu'à F_{10}.
2. Montrer que pour tout entier non nul n,
$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.
3. En déduire que pour tout entier non nul n, $F_n \wedge F_{n+1} = 1$.
4. Soit n un entier non nul. Montrer par récurrence sur l'entier m que $F_{n+m} = F_m F_{n-1} + F_{m+1} F_n$.
5. En déduire que $F_m \wedge F_n = F_m \wedge F_{m+n}$.

31 Pour tout entier naturel n, on note $\varphi(n)$ le nombre d'entier naturels inférieurs à n et premiers avec n.
On pose $\varphi(1) = 1$.
1. Vérifier que $\varphi(7) = 6$ et $\varphi(8) = 4$.
2. Montrer que $\varphi(n) \leq n - 1$.
Soit k un entier naturel non nul, p et q deux nombres premiers et a un entier non divisible par p et q.
3. a. Montrer que $\varphi(p) = p - 1$.
b. Montrer que $a^{\varphi(p)} \equiv 1 \pmod{p}$.
4. a. Montrer que $\varphi(pq) = \varphi(p)\varphi(q)$.
b. Montrer que $a^{\varphi(pq)} \equiv 1 \pmod{pq}$.
c. En déduire les congruences ci-dessous
$10^{1536} \equiv 1 \pmod{1649}$;
$10430^{10200} \equiv 1 \pmod{10403}$.
5. a. Montrer que $\varphi(p^k) = p^k - p^{k-1}$.
b. Déterminer $\varphi(125)$, $\varphi(256)$ et $\varphi(1331)$.
6. a. Montrer que $(1+up)^{p^{k-1}} \equiv 1 \pmod{p^k}$
(On pourra utiliser que tout entier non nul n divise C_n^j, $j \neq 0$ et $j \neq n$).
b. Montrer que $a^{\varphi(p^k)} \equiv 1 \pmod{p^k}$.
En déduire les congruences ci-dessous
$17^{100} \equiv 1 \pmod{125}$; $17^{128} \equiv 1 \pmod{256}$.

Qarray.tn-Aqra Blech-Qarray.tn